

FIG.1

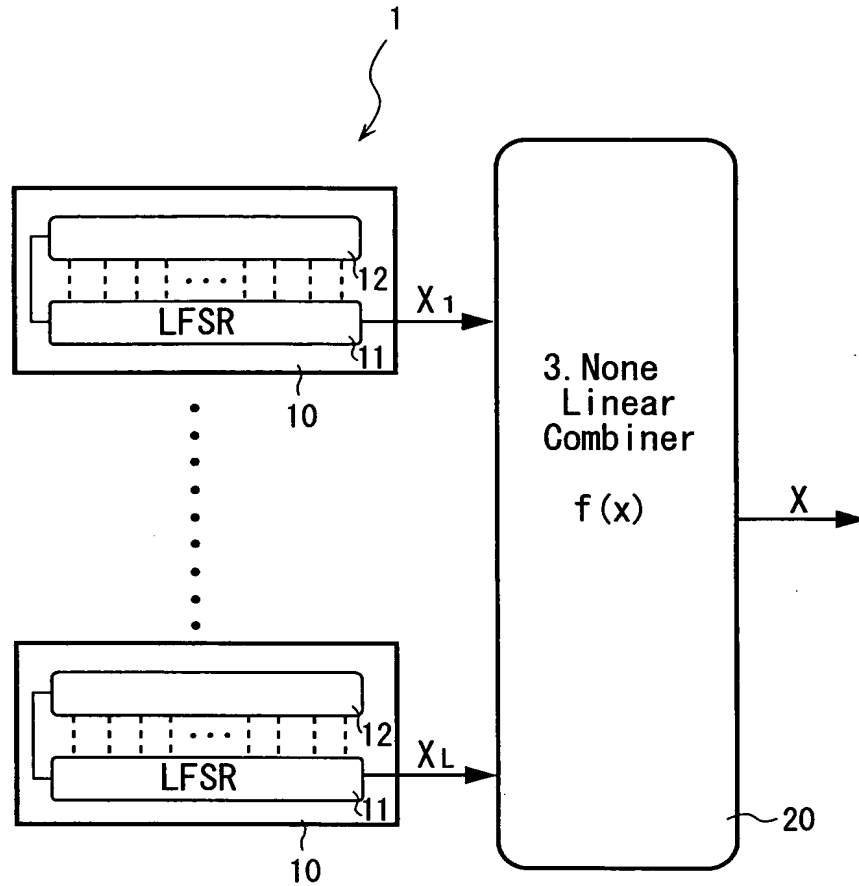


FIG.2

LSFR1	$x^{131} + x^8 + x^3 + x^2 + 1$
LSFR2	$x^{137} + x^{21} + 1$
LSFR3	$x^{139} + x^8 + x^5 + x^3 + 1$
LSFR4	$x^{149} + x^{10} + x^9 + x^7 + 1$
LSFR5	$x^{151} + x^3 + 1$
LSFR6	$x^{157} + x^6 + x^5 + x^2 + 1$
LSFR7	$x^{163} + x^7 + x^6 + x^3 + 1$
LSFR8	$x^{167} + x^6 + 1$

FIG. 3

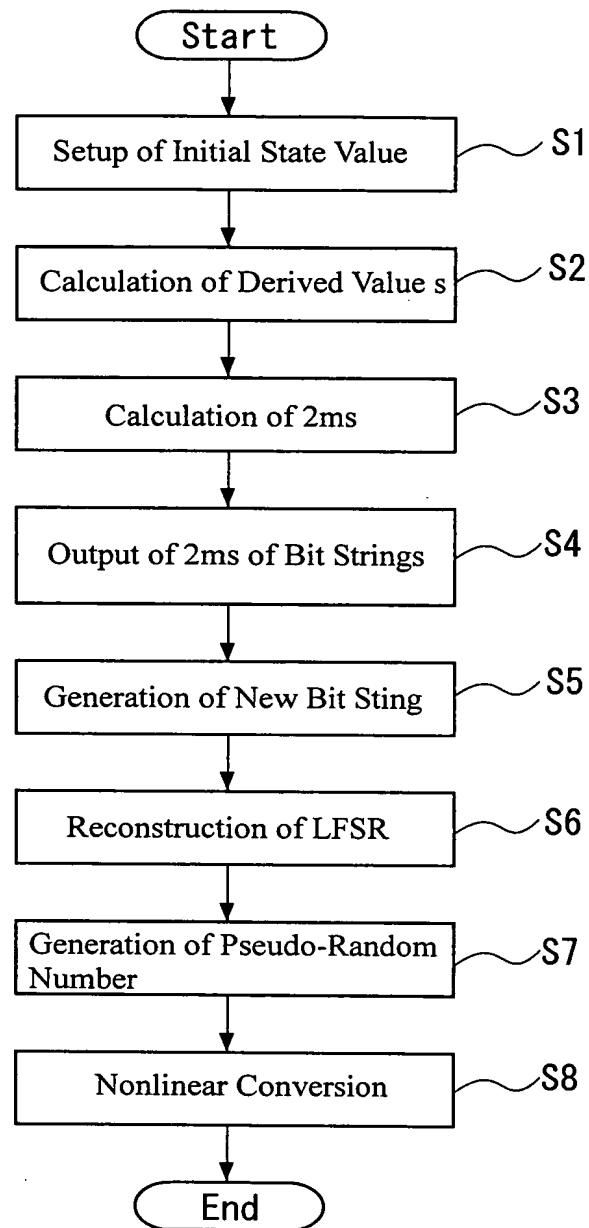


FIG. 4

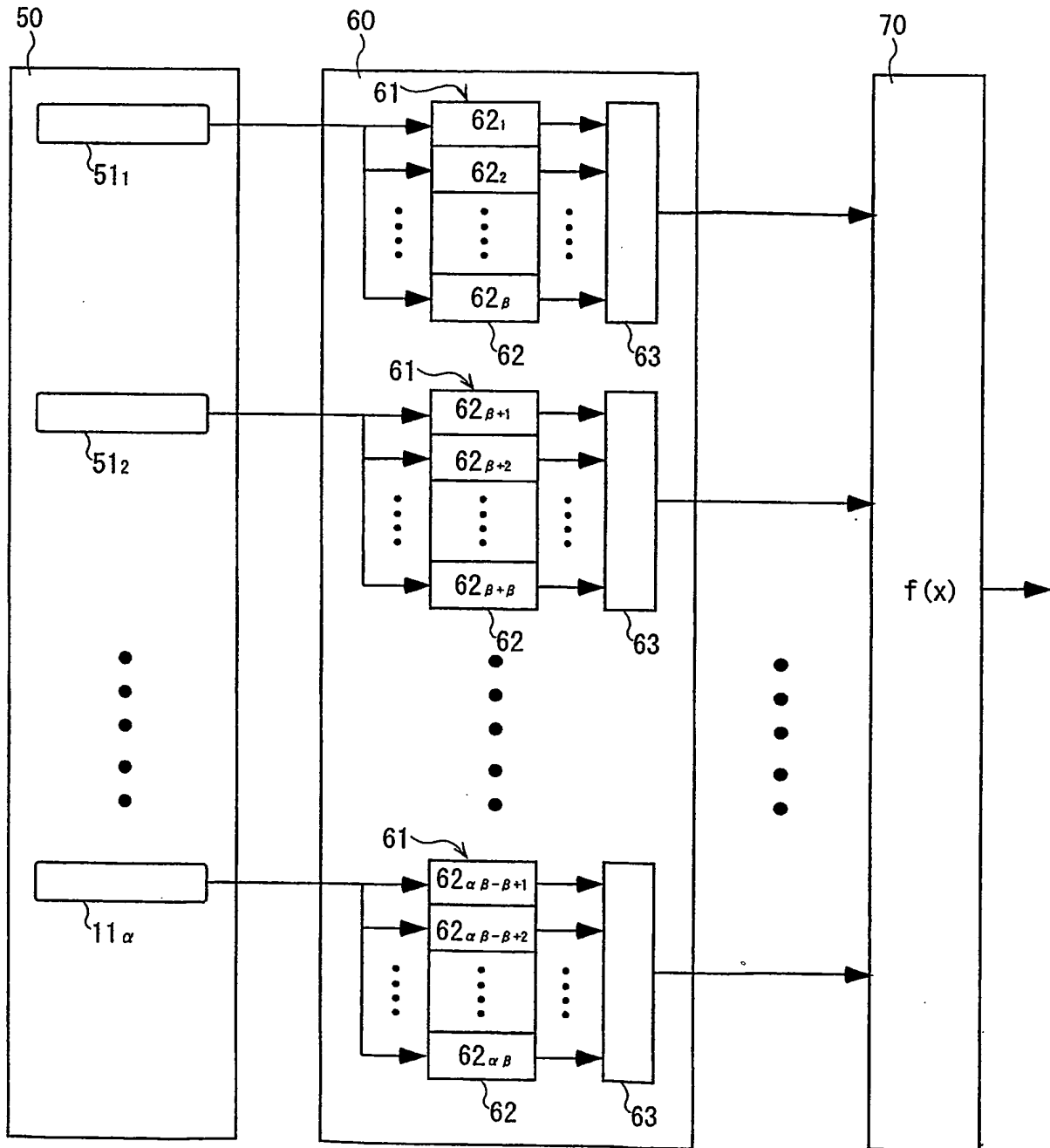


FIG. 5

Ri		Ro	
2 ^{Ni}	000	01001110010100100010100
	001	00101001101000111001010
	002	00011100101000011011110
	003	01001100011110000101111
	⋮		⋮
Ni Bits		No Bits	

FIG. 6

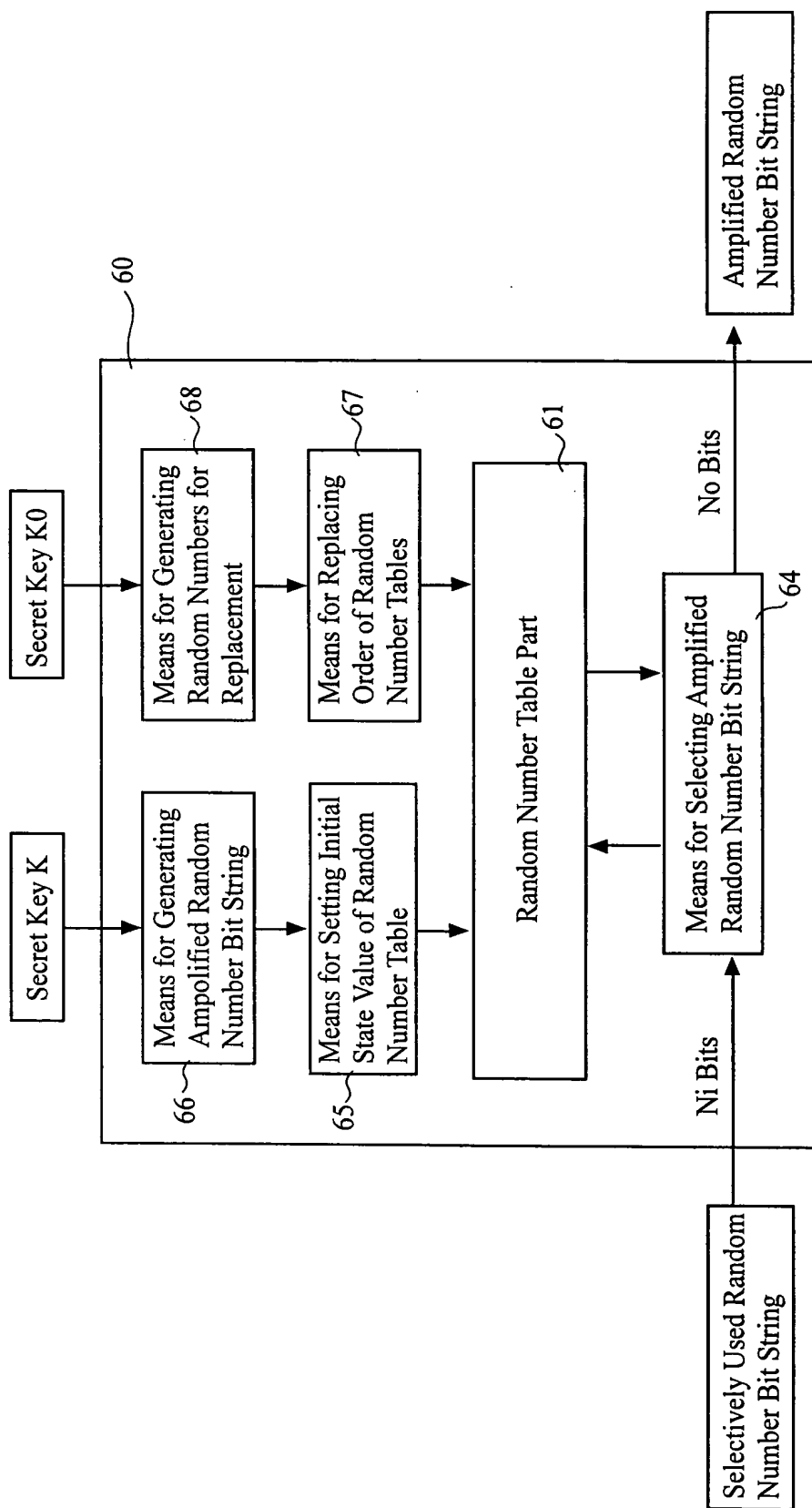


FIG. 7

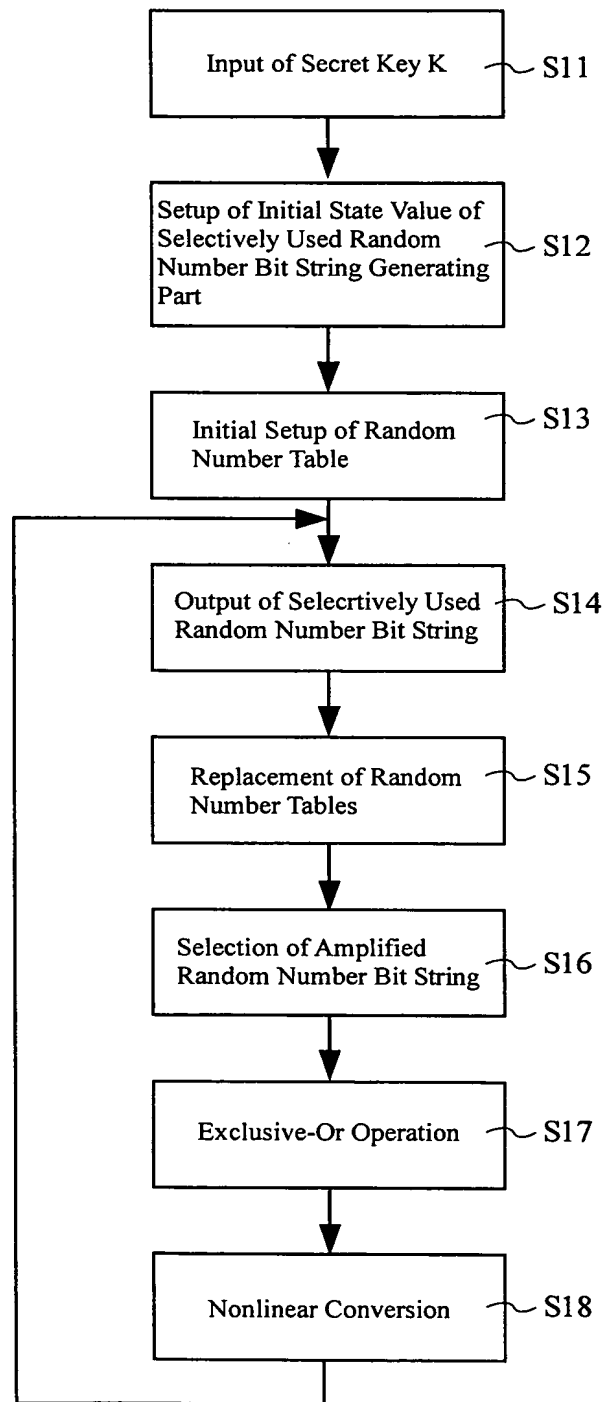


FIG. 8

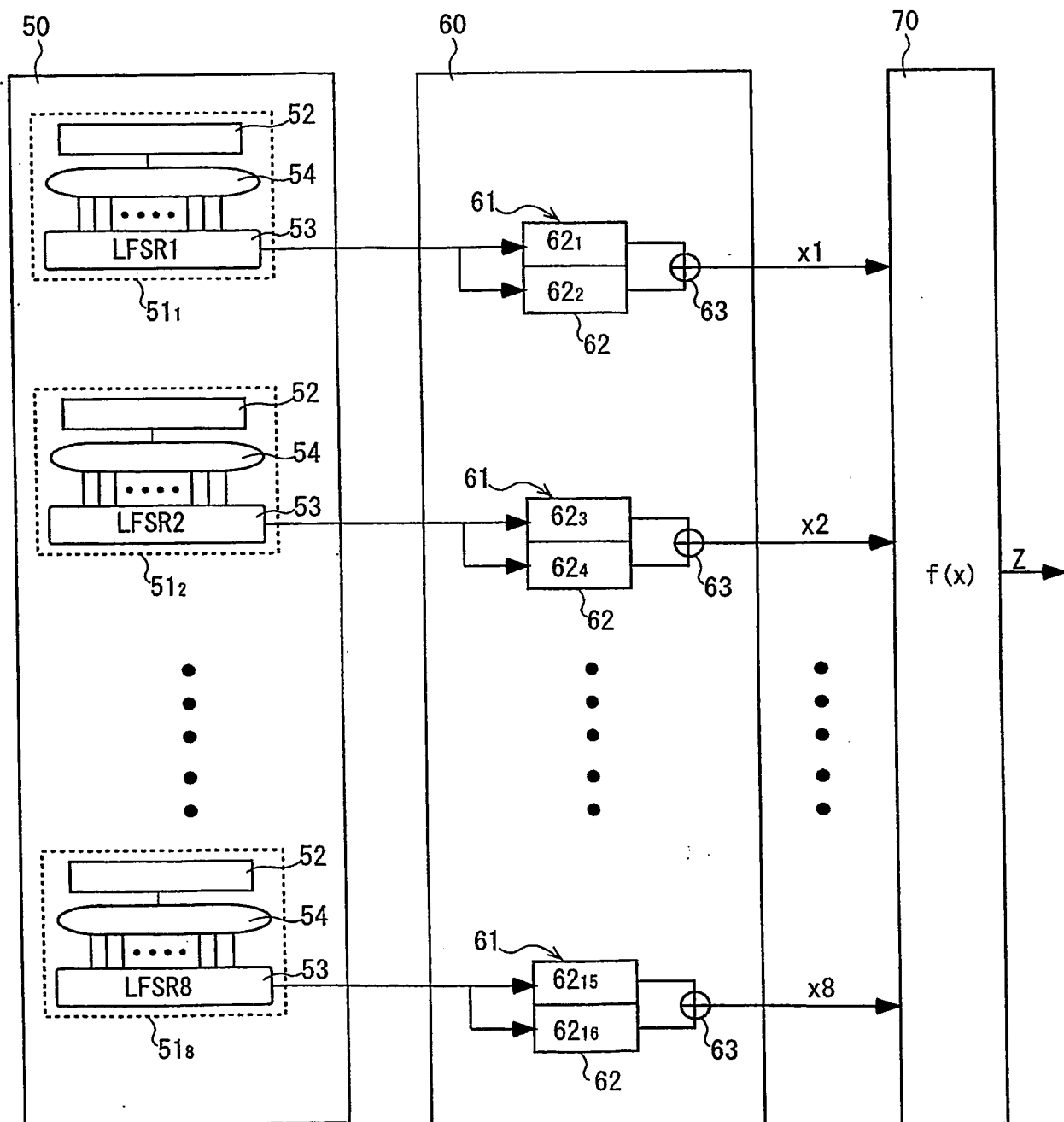


Fig. 9

In case of $\alpha = 8$, $\beta = 2$, $N_i = 2^{16}$, $L_k = 128$

Selectively Used Random Number Bit String
Corresponding to Output Means 61₁

Selectively Used Random Number Bit String
Corresponding to Output Means 61₂

Selectively Used Random Number Bit String
Corresponding to Output Means 61_n

R _i	R _o
0	010110101100010110
1	101101011000101100
2	101011010110001011
3	010110101101110110
.	.
.	.
.	.
255	010110100010101010
0	001010101100010110
1	101011101000101100
2	000101101011010111
3	011011010110101101
.	.
.	.
.	.
255	001010110101100110
0	101010010010101010
1	101101011000101110
2	111010100110001011
3	010110110101011011
.	.
.	.
.	.
255	110101101000010110
0	100010110010110101
1	001011100010110101
2	010110101100101011
3	001101011010110111
.	.
.	.
.	.
255	110100101101010010
	↪
0	010011011010110001
1	010110110101100100
2	110001011010110110
3	011011100111010110
.	.
.	.
.	.
255	010101101100011001
0	110110110111001010
1	100110110111011100
2	011010101110011010
3	011011010111011001
.	.
.	.
.	.
255	010101010110001101

FIG.10

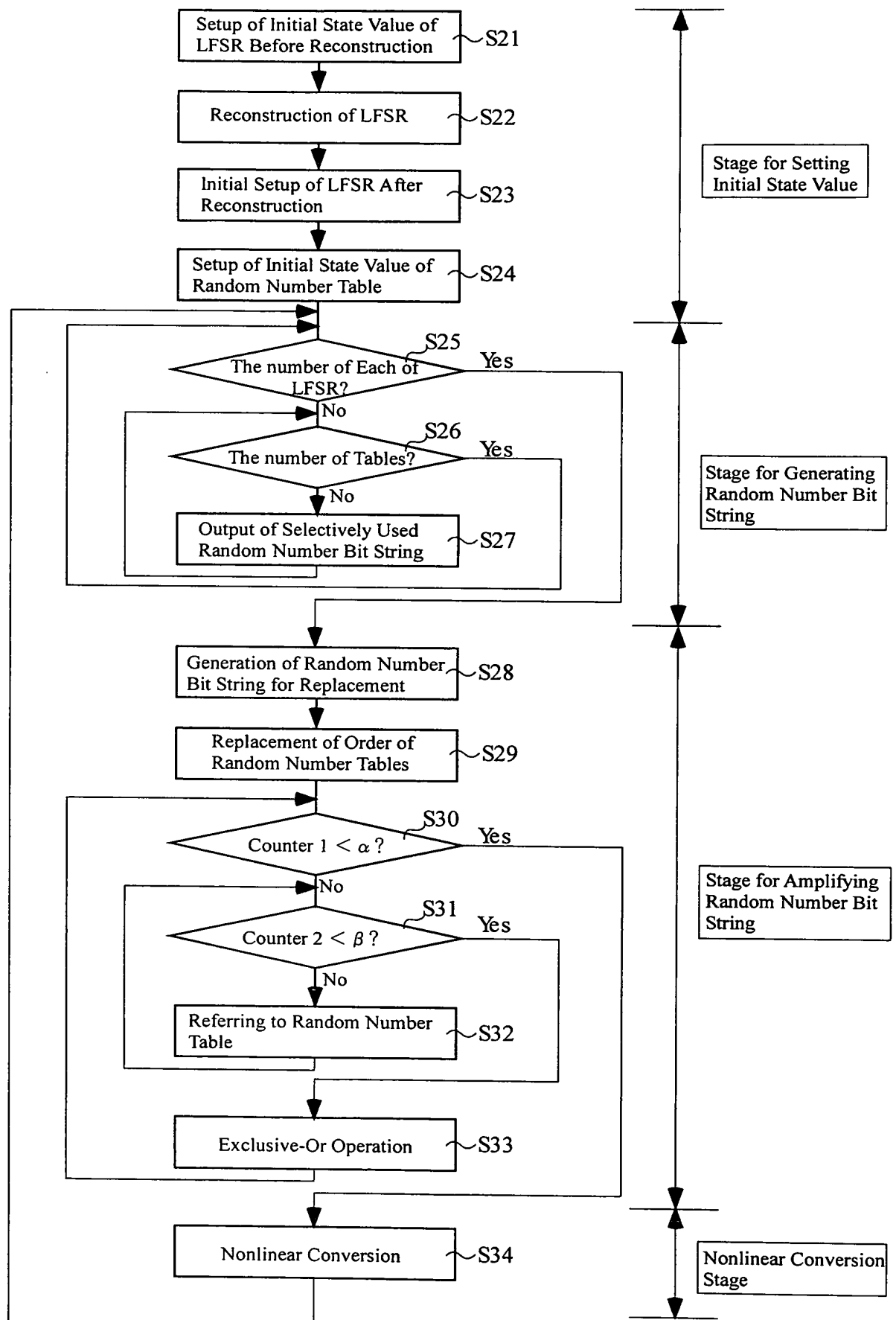


FIG.11

LFSR1	$I1(x) = x^{129} + x^{80} + x^8 + x + 1$
LFSR2	$I2(x) = x^{131} + x^{80} + x^{16} + x + 1$
LFSR3	$I3(x) = x^{133} + x^{16} + x^8 + x^2 + 1$
LFSR4	$I4(x) = x^{137} + x^{20} + x^{12} + x + 1$
LFSR5	$I5(x) = x^{139} + x^{80} + x^{12} + x + 1$
LFSR6	$I6(x) = x^{143} + x^{56} + x^{12} + x + 1$
LFSR7	$I7(x) = x^{149} + x^{84} + x^8 + x^2 + 1$
LFSR8	$I8(x) = x^{151} + x^{60} + x^8 + x + 1$

FIG.12

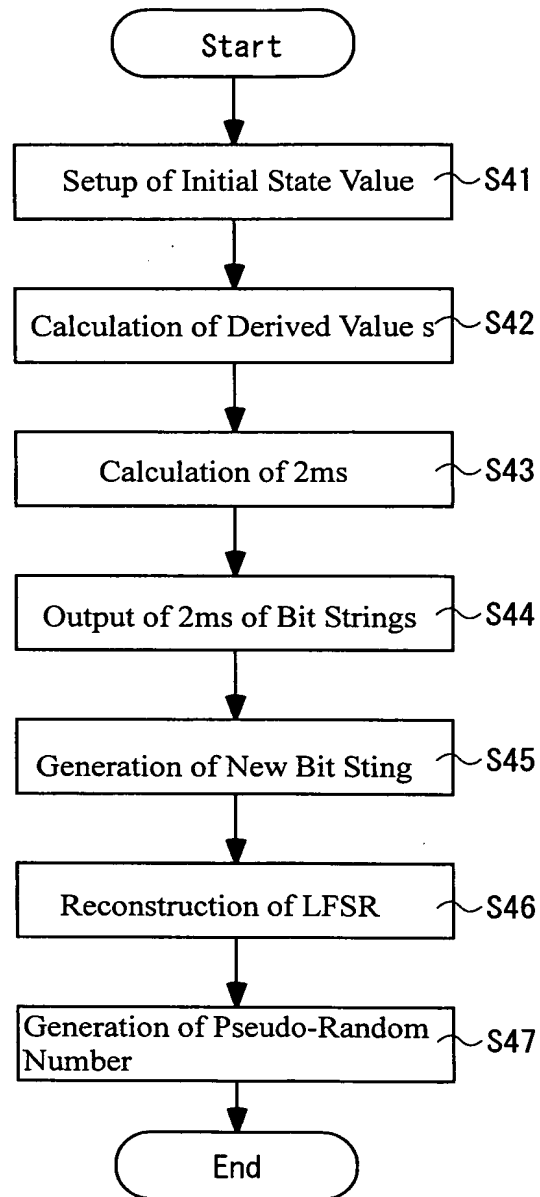


FIG.13

Table 1: Throughput Measurement Result

Means Throughput of LFSR (151 Lines)	5.203Mbits/sec
Mean Throughput of RC4	141.6Mbits/sec
Mean Throughput of Replacement Processing	69.99Mbits/sec
Mean Throughput of Random Number Table	7.923Gbits/sec
Mean Throughput of Nonlinear Function	119.2Mbits/sec
Throughput of Whole Pseudo-Random Number Generator	116.4Mbits/sec
Mean Throughput of Conventional Type	0.680Mbits/sec

FIG.14

Table 2: Parameter of NIST

Data Length	1,000,000
Block Frequency Test Block Length	100
Non Overlapping Template Test Block Length	10
Overlapping Template Test Block Length	10
Universal Test Block Length	7
Universal Test Number Of Initialization Steps	1,280
Approximate Entropy Test Block Length	2
Serial Test Block Length	2
Linear Complexity Test Subsequence Length	500
bitstreams should be generated	10

FIG.15

Test Items	P-value	Test Items	P-value	Test Items	P-value	Test Items	P-value
Frequency	0.987896	Aperiodic-Template	0.657933	Aperiodic-Template	0.616305	Random-Excursion-V	0.035174
Block-Frequency	0.678686	Aperiodic-Template	0.494392	Aperiodic-Template	0.042808	Random-Excursion-V	0.911413
Cusum	0.366918	Aperiodic-Template	0.987896	Aperiodic-Template	0.759756	Random-Excursion-V	0.350485
Cusum	0.213309	Aperiodic-Template	0.419021	Aperiodic-Template	0.779188	Random-Excursion-V	0.534146
Runs	0.383827	Aperiodic-Template	0.350485	Aperiodic-Template	0.262249	Random-Excursion-V	0.350485
Long-Run	0.595549	Aperiodic-Template	0.616305	Aperiodic-Template	0.455937	Random-Excursion-V	0.213309
Rank	0.798139	Aperiodic-Template	0.935716	Aperiodic-Template	0.55442	Random-Excursion-V	0.213309
FFT	0.021999	Aperiodic-Template	0.897763	Aperiodic-Template	0.383827	Random-Excursion-V	0.534146
Aperiodic-Template	0.867692	Aperiodic-Template	0.897763	Aperiodic-Template	0.12962	Random-Excursion-V	0.534146
Aperiodic-Template	0.574903	Aperiodic-Template	0.171867	Aperiodic-Template	0.867692	Random-Excursion-V	0.122325
Aperiodic-Template	0.779188	Aperiodic-Template	0.739918	Aperiodic-Template	0.759756	Random-Excursion-V	0.213309
Aperiodic-Template	0.350485	Aperiodic-Template	0.897763	Aperiodic-Template	0.637119	Random-Excursion-V	0.066882
Aperiodic-Template	0.798139	Aperiodic-Template	0.224821	Aperiodic-Template	0.867692	Random-Excursion-V	0.035174
Aperiodic-Template	0.494392	Aperiodic-Template	0.851383	Aperiodic-Template	0.955835	Serial	0.350485
Aperiodic-Template	0.867692	Aperiodic-Template	0.419021	Aperiodic-Template	0.897763	Serial	0.289667
Aperiodic-Template	0.085587	Aperiodic-Template	0.319084	Aperiodic-Template	0.996335	Lempel-Ziv	0.383827
Aperiodic-Template	0.474986	Aperiodic-Template	0.401199	Aperiodic-Template	0.115387	Linear-Complexity	0.090936
Aperiodic-Template	0.996335	Aperiodic-Template	0.616305	Aperiodic-Template	0.383827		
Aperiodic-Template	0.249284	Aperiodic-Template	0.911413	Aperiodic-Template	0.275709		
Aperiodic-Template	0.153763	Aperiodic-Template	0.897763	Aperiodic-Template	0.55442		
Aperiodic-Template	0.514124	Aperiodic-Template	0.897763	Aperiodic-Template	0.051942		
Aperiodic-Template	0.657933	Aperiodic-Template	0.897763	Aperiodic-Template	0.595549		
Aperiodic-Template	0.595549	Aperiodic-Template	0.080519	Aperiodic-Template	0.657933		
Aperiodic-Template	0.719747	Aperiodic-Template	0.867692	Aperiodic-Template	0.637119		
Aperiodic-Template	0.996335	Aperiodic-Template	0.115387	Aperiodic-Template	0.045675		
Aperiodic-Template	0.657933	Aperiodic-Template	0.275709	Aperiodic-Template	0.924076		
Aperiodic-Template	0.759756	Aperiodic-Template	0.779188	Aperiodic-Template	0.978072		
Aperiodic-Template	0.834308	Aperiodic-Template	0.202268	Aperiodic-Template	0.739918		
Aperiodic-Template	0.851383	Aperiodic-Template	0.319084	Aperiodic-Template	0.455937		
Aperiodic-Template	0.657933	Aperiodic-Template	0.637119	Aperiodic-Template	0.657933		
Aperiodic-Template	0.494392	Aperiodic-Template	0.739918	Aperiodic-Template	0.574903		
Aperiodic-Template	0.779188	Aperiodic-Template	0.224821	Aperiodic-Template	0.304126		
Aperiodic-Template	0.883171	Aperiodic-Template	0.514124	Aperiodic-Template	0.249284		
Aperiodic-Template	0.798139	Aperiodic-Template	0.137282	Aperiodic-Template	0.289667		
Aperiodic-Template	0.719747	Aperiodic-Template	0.964295	Aperiodic-Template	0.946308		
Aperiodic-Template	0.964295	Aperiodic-Template	0.334538	Aperiodic-Template	0.010535		
Aperiodic-Template	0.401199	Aperiodic-Template	0.678686	Aperiodic-Template	0.816537		
Aperiodic-Template	0.12962	Aperiodic-Template	0.719747	Aperiodic-Template	0.739918		
Aperiodic-Template	0.739918	Aperiodic-Template	0.080519	Aperiodic-Template	0.350485		
Aperiodic-Template	0.010555	Aperiodic-Template	0.145326	Aperiodic-Template	0.798139		
Aperiodic-Template	0.202268	Aperiodic-Template	0.319084	Aperiodic-Template	0.455937		
Aperiodic-Template	0.289667	Aperiodic-Template	0.145326	Aperiodic-Template	0.145326		
Aperiodic-Template	0.897763	Aperiodic-Template	0.304126	Periodic-Template	0.657933		
Aperiodic-Template	0.719747	Aperiodic-Template	0.867692	Universal	0.383827		
Aperiodic-Template	0.494392	Aperiodic-Template	0.719747	Apen	0.534146		
Aperiodic-Template	0.019188	Aperiodic-Template	0.437274	Random-Excursion	0.534146		
Aperiodic-Template	0.066882	Aperiodic-Template	0.030806	Random-Excursion	0.213309		
Aperiodic-Template	0.574903	Aperiodic-Template	0.224821	Random-Excursion	0.534146		
Aperiodic-Template	0.699313	Aperiodic-Template	0.514124	Random-Excursion	0.035174		
Aperiodic-Template	0.978072	Aperiodic-Template	0.171867	Random-Excursion	0.534146		
Aperiodic-Template	0.153763	Aperiodic-Template	0.010988	Random-Excursion	0.534146		
Aperiodic-Template	0.419021	Aperiodic-Template	0.946308	Random-Excursion	0.010879		
Aperiodic-Template	0.851383	Aperiodic-Template	0.162606	Random-Excursion	0.213309		
Aperiodic-Template	0.55442	Aperiodic-Template	0.534146	Random-Excursion-V	0.534146		
Aperiodic-Template	0.897763	Aperiodic-Template	0.574903	Random-Excursion-V	0.739918		
Aperiodic-Template	0.213309	Aperiodic-Template	0.334538	Random-Excursion-V	0.213309		
Aperiodic-Template	0.319084	Aperiodic-Template	0.699313	Random-Excursion-V	0.911413		

FIG. 16

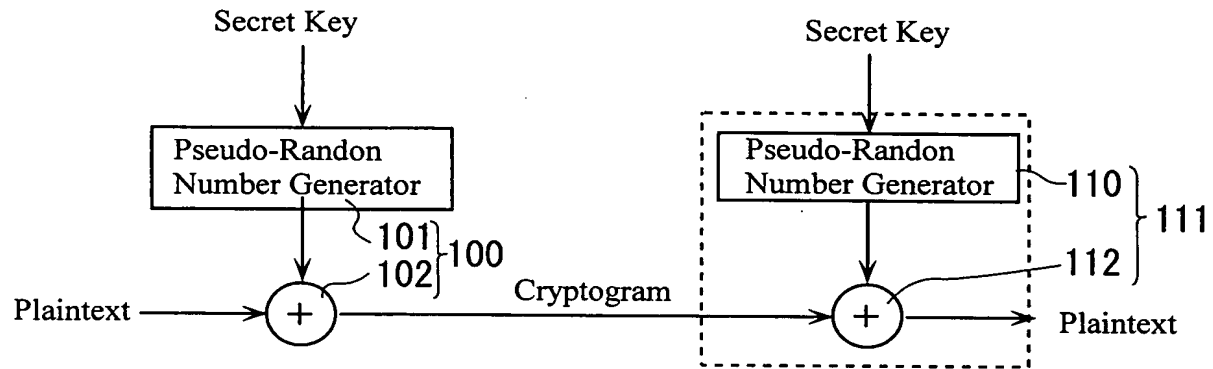


FIG. 17

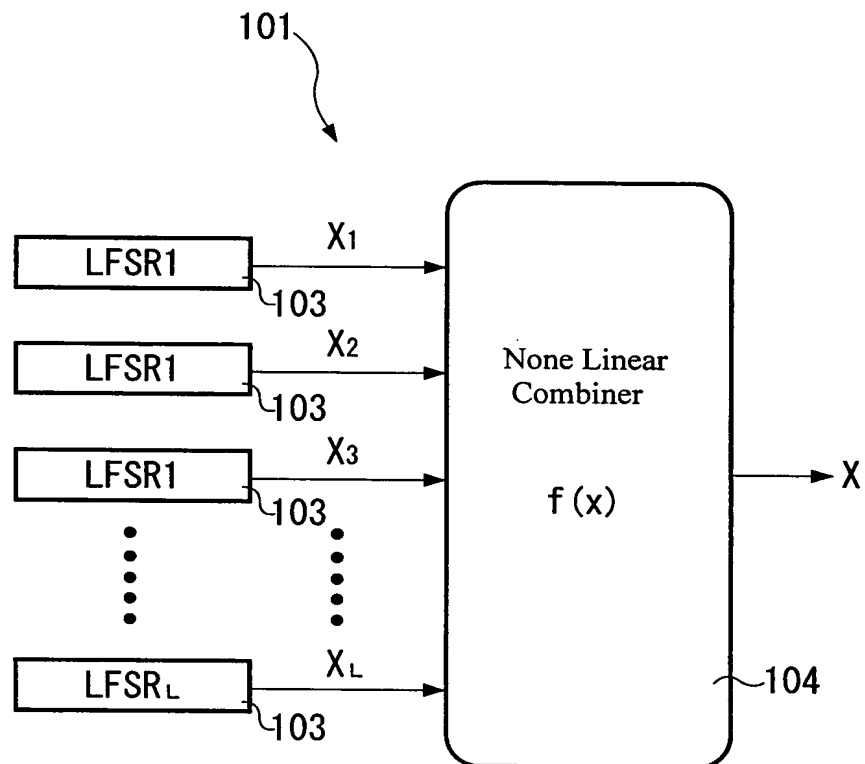


FIG. 18

